Zasady przetwarzania danych osobowych

Przy przetwarzaniu danych osobowych w zgodzie z RODO należy przestrzegać określonych zasad:

- zgodności z prawem, rzetelności i przejrzystości – mówiącej, że przetwarzanie musi odbywać się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- ograniczenia celu – nakazującej zbieranie danych jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie ich w sposób niezgodny z tymi celami;
- adekwatności – nakazującej zbierać tylko te dane, które są niezbędne do osiągnięcia celu, w jakim zostały zebrane;
- minimalizacji – wynikającej z zasady adekwatności i dotyczącej minimalizacji ilości zbieranych danych do tego, co niezbędne do celów przetwarzania;
- prawidłowości – nakazującej dbałość o to, by dane były prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- ograniczenia przechowywania – stanowiącej, że przechowywanie danych musi odbywać się w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
- integralności i poufności – mówiącej o przetwarzaniu danych w sposób zapewniający odpowiednie bezpieczeństwo, w tym ich ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem. Administrator danych ma obowiązek zabezpieczyć przetwarzane dane za pomocą odpowiednich środków technicznych lub organizacyjnych.

Czym jest naruszenie ochrony danych osobowych?

Jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Incydenty przy przetwarzaniu danych osobowych można podzielić na:

- **incydent umyślny** (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń);
- **zdarzenie losowe wewnętrzne** (np. awaria komputera/serwera/dysku, błędy użytkowników, utrata danych);
- **zdarzenie losowe zewnętrzne** (np. pożar, zalanie wodą, utrata zasilania, utrata łączności);
- **incydenty wynikające z zagrożeń naturalnych** (zjawiska klimatyczne, korozja, promieniowanie).

Odpowiedzialność ADO za przetwarzane dane

Uniwersytet Zielonogórski jako Administrator Danych (ADO) przetwarzając dane w ramach prowadzonej działalności ponosi pełną odpowiedzialność za stan bezpieczeństwa przetwarzanych danych, do których uzyska dostęp w związku z realizacją powierzonych obowiązków. ADO jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych stosowną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Odpowiedzialność za naruszenie RODO ma charakter odpowiedzialności administracyjnoprawnej oraz cywilnoprawnej. Każda osoba, która poniosła szkodę w wyniku naruszenia postanowień RODO ma prawo wystąpić do ADO z roszczeniem o odszkodowanie za poniesioną szkodę. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym RODO. Administrator może zostać zwolniony z odpowiedzialności wynikającej z naruszenia ochrony danych, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Kary administracyjne

Ustawodawca unijny zadbał, by wynikające z naruszeń RODO kary były skuteczne, proporcjonalne i odstraszające. Administracyjne kary pieniężne nakładane są po rozpatrzeniu indywidualnie każdego przypadku.

Organ nadzorczy - Prezes Urzędu Ochrony Danych zgodnie z Ustawą o ochronie danych osobowych z dnia 25 maja 2018 r.- decydując o nałożeniu administracyjnej kary pieniężnej oraz o jej wysokości bierze pod uwagę między innymi:

- charakter (umyślny lub nieumyślny);
- wagę i czas trwania naruszenia, działania podjęte przez administratora minimalizujące szkodę poniesioną przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora uwzględniający środki techniczne i organizacyjne wdrożone przez ADO;
- wcześniejsze naruszenia ze strony administratora;
- współpracę z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego skutków;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, czy administrator zgłosił naruszenie;
- stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji.

Rozporządzenie reguluje ogólne warunki nakładania administracyjnych kar pieniężnych i wyróżnia dwa przedziały kar dla ADO:

- **do 10 mln euro**, a w przypadku przedsiębiorcy – alternatywnie do 2 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Kara ta dotyczy naruszeń związanych między innymi z niewywiązaniem się przez ADO ze swoich obowiązków takich jak: obowiązek informacyjny, brak uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych, błędnie prowadzony rejestr czynności przetwarzania lub jego brak, nieprawidłowe zabezpieczenie systemów informatycznych, nieprzeprowadzenie oceny skutków dla ochrony danych, brak powołania Inspektora Ochrony Danych jeśli istniał taki obowiązek;
- **do 20 mln euro**, a w przypadku przedsiębiorcy – alternatywnie do 4 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Kara ta dotyczy między innymi następujących naruszeń: złamania przez ADO podstawowych zasad przetwarzania danych osobowych, w tym niedopilnowanie warunków pozyskania zgody, łamania praw osób, których dane dotyczą, nieprawidłowego przekazywania danych osobowych odbiorcom w państwach trzecich lub organizacjach międzynarodowych.

Przepisy krajowe (powiązane z RODO) o karach administracyjnych

W ustawie o ochronie danych osobowych z dnia 25 maja 2018 r.-kary dla podmiotów publicznych, między innymi dla uczelni publicznych, wynoszą do 100 tys. złotych.